FCC Federal Communications Commission

BROADBAND.GOV
NATIONAL BROADBAND PLAN

Public Safety and the National Broadband Plan

Jennifer A. Manner

Framework for Recommendations

1 Creating a nationwide interoperable broadband wireless public safety network

2 Transitioning to a next-generation 9-1-1 system

3 Developing a comprehensive next-generation alerting system

4 Enhancing security measures to safeguard networks and core infrastructure

Nationwide Interoperable Public Safety Wireless Broadband Network

Benefits of Incentive-Based Partnership Approach

- Increased redundancy and reliability
- Improved capacity and performance for Public Safety
- Reduced costs for PS agencies and state and local governments
- Improves commercial infrastructure and reach
- Transition path to increased spectrum and operational efficiency
- Enable public safety to evolve with commercial technology, applications, and devices improvements (evergreen)

Broadband Network Strategy

Vision: For significantly less then what has been spent on narrowband interoperability, a new interoperable broadband network will be deployed using commercial technologies, bringing public safety communications into the 21st Century

Administrative and Technical Regime

- Authorized network operators will deploy and operate the PS BB network in partnership with commercial entities (RFP approach) (or on their own)
- PS access to roaming and priority access on commercial networks
- Improves redundancy and resiliency
- D block licensed for commercial user
- Competitive options for incentive- based partnerships
- User device requirements

ERIC

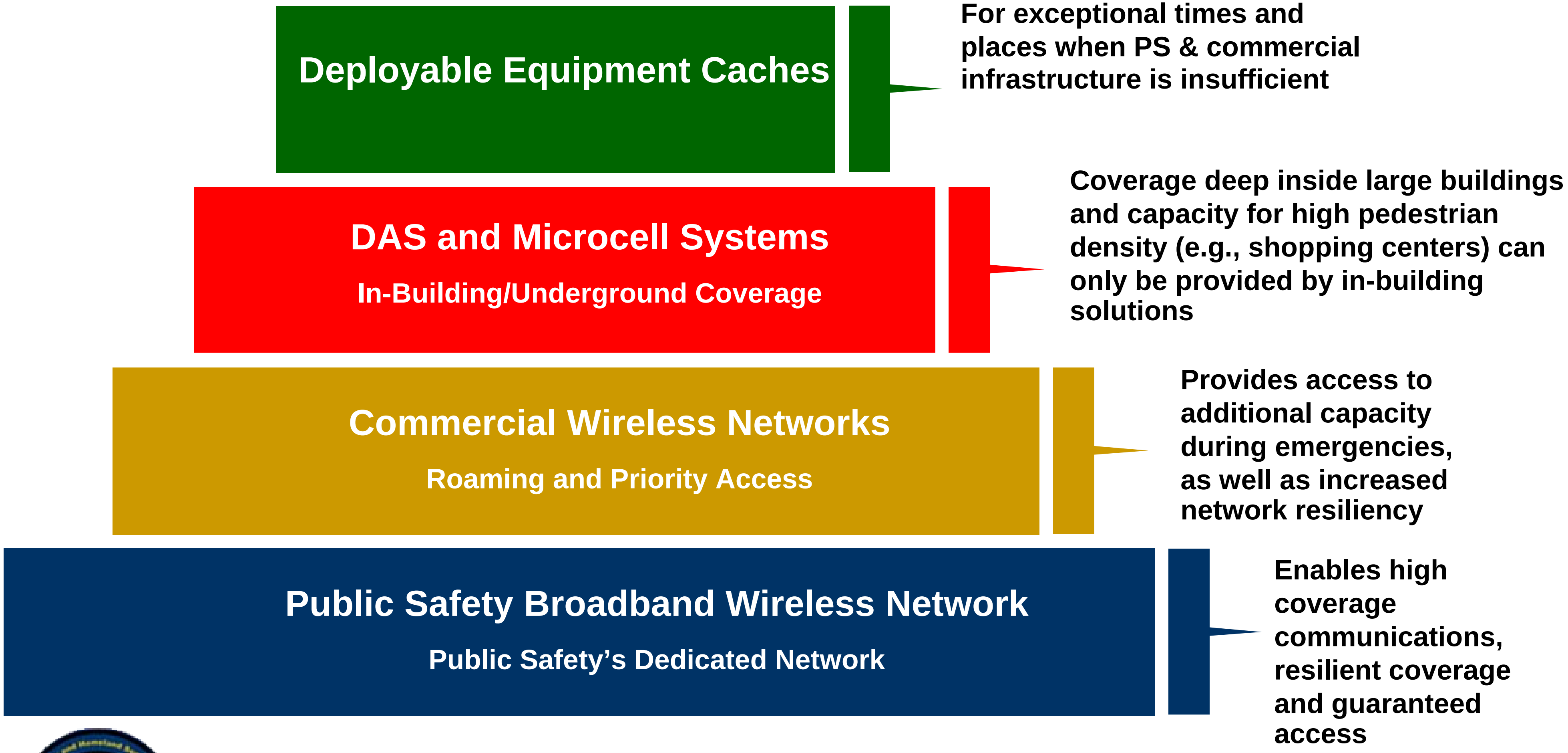
- Establish framework for interoperability and operability requirements
- Avoids fragmented networks of the past

Funding

- Fund network construction, operation, and evolution
- Nationwide availability
- Hardened network
- Cap Ex Public Funding
- Op Ex Public Funding

Public Safety Network and Solutions

Solution for Reliable, High Coverage Mission Critical Voice, Data, & Video 4G Services



Deployable Equipment Caches

For exceptional times and places when PS & commercial infrastructure is insufficient

DAS and Microcell Systems

In-Building/Underground Coverage

Coverage deep inside large buildings and capacity for high pedestrian density (e.g., shopping centers) can only be provided by in-building solutions

Commercial Wireless Networks

Roaming and Priority Access

Provides access to additional capacity during emergencies, as well as increased network resiliency

Public Safety Broadband Wireless Network

Public Safety's Dedicated Network

Enables high coverage communications, resilient coverage and guaranteed access

Next-Generation 9-1-1

Next Generation 9-1-1 Current Status

- The process of transitioning from the legacy 9-1-1 system to NG9-1-1 has begun.
- Public safety and industry standards organizations have arrived at a consensus on NG9-1-1 technical architecture to meet the demands posed by new technology and methods of communication.
- The Department of Transportation (DOT) has published a transition plan for NG9-1-1 migration.
- A few states and localities have begun deployment of NG9-1-1, and there is at least one live test of 9-1-1 texting on-going.
- Existing regulatory roadblocks hinder NG9-1-1 deployment and existing grant programs are uncoordinated and limited in scope.

Next Generation 9-1-1 Recommendations in NBP

- The National Highway Traffic Safety Administration (NHTSA) should direct a report that analyzes the costs of deploying a NG9-1-1 system on a nationwide basis.
- Congress should use the NHTSA report as a resource for establishing a NG9-1-1 funding mechanism.
- Congress should consider restoring the E911 Implementation Coordination Office to help deploy NG9-1-1.
- Congress should enact legislation to establish a federal regulatory framework for development of NG9-1-1 and the transition from legacy 9-1-1 to NG9-1-1 networks over time.
- FCC should issue a Further Notice of Proposed Rulemaking to explore how NG9-1-1 may impact location accuracy requirements.
- In effort to meet the public's expectations, the FCC should initiate a Notice of Inquiry that would address the future roles of 9-1-1 and NG9-1-1 as communications technologies, networks and architectures expand beyond traditional voice-centric devices.

Next-Generation Alerting

Next Generation Alerting NOI

- Comprehensive inquiry into all issues associated with developing a multi-platform, redundant, broadband-based next generation alert system.
- Will examine:
  - Potential multi-platform technologies, including the Internet.
  - Developments in current alerting systems such as EAS, CMAS and IPAWS
  - Needs of state, tribal and local governments in utilizing the next generation alerting system

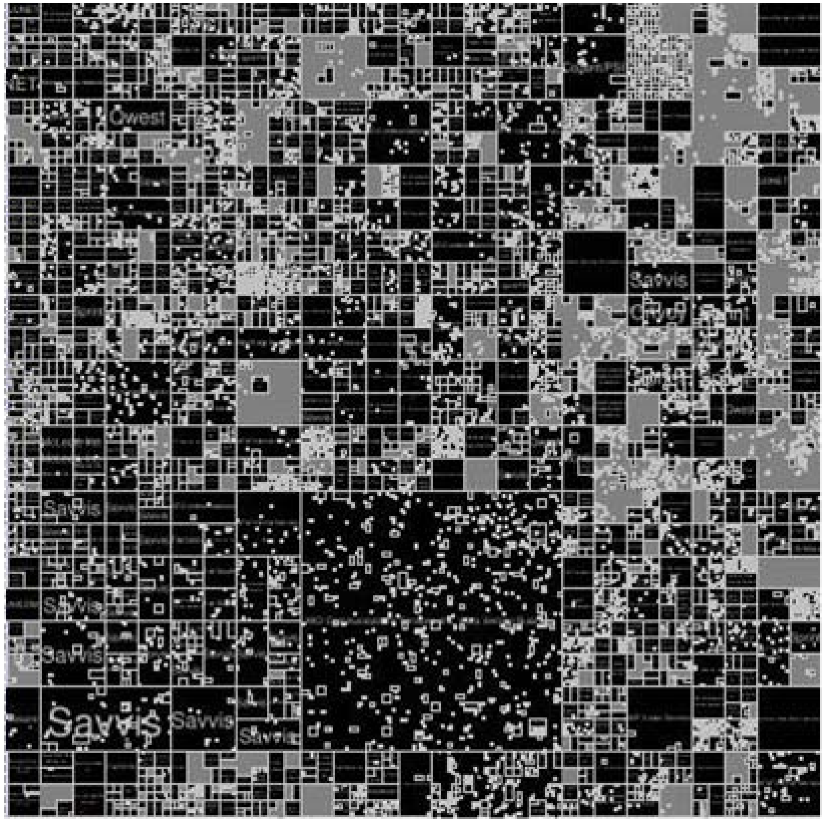
Federal Agency Roles in Next Generation Alerting

- Executive Branch should take action to:
  - Clarify responsibilities of each federal agency with respect to next generation alerting
  - Set milestones, benchmarks and actions for system implementation
  - Establish system of accountability among federal agencies responsible for emergency alerting.

Cyber Security / Critical Infrastructure

Cyber Security Roadmap

- Develop and issue a roadmap to address cybersecurity in coordination with the Executive Office of the President
  - Identify the five most critical cyber security threats:
  - Establish a two-year plan, including milestones, for the FCC to address these threats.



Cyber Security Recommendations

- Expand FCC Outage Reporting Requirements To Broadband ISPs
  - The FCC is planning to initiate a proceeding to extend FCC Part 4 outage reporting rules to broadband on Internet Service Providers (ISPs) and interconnected VoIP providers in late 2010 .
  - Reports from such entities will allow the FCC, other federal agencies and, as appropriate, service providers to analyze information on outages affecting IP-based networks, prevent future outages, and ensure a better response to outages that do occur.
- Voluntary Cyber security Certification
  - The FCC, in April 2010, will begin a proceeding to establish a voluntary cyber security certification system that creates market incentives for communications service providers to upgrade the cyber-security measures they use on their networks and examine additional voluntary incentives that could improve cyber security as well improve education about cyber security issues.
  - A voluntary cyber security certification program should promote more vigilant network security among market participants, increase the security of the nation's communications infrastructure, and offer end users more complete information about their providers' cyber security practices.
- Cyber security Information Reporting System
  - The FCC and DHS' Office of Cyber security and Communications together should develop an IP network Cyber security Information Reporting System (CIRS) to gather and disseminate information rapidly to participating providers during major cyber events.
    - CIRS should be crafted as a real-time voluntary monitoring system for cyber events affecting the communications infrastructure.

Critical Infrastructure Recommendations

- Network Resilience and Preparedness
  - In April 2010 the FCC will begin an inquiry into the resilience of broadband networks under a set of physical failures —either malicious or non-malicious.
    - This will allow the FCC to assess the ability of broadband networks. including next-generation public safety communications networks, to withstand direct attacks and determine if any actions should be taken in this regard.
    - This will identify the major single points of failure in broadband networks and identify situations where existing redundancy may not be working as intended.

  - This proceeding will also examine commercial networks' preparedness to withstand severe overloads that may occur during extraordinary events, such as bioterrorism attacks or pandemics. Proceeding will give the FCC information in the following areas:
    - Susceptibility of such networks to severe overloads and the adequacy of current network management techniques to handle these overloads.
    - The advisability and need for traffic prioritization to handle severe overloads.

Critical Infrastructure Recommendations

- Priority Network Access and Routing
  - The FCC and the National Communications System (NCS) will leverage their experience with the Government Emergency Telecommunications Service (GETS) and the WPS to jointly develop a system of priority network access and traffic routing for national security/emergency preparedness (NS/EP) users on broadband communications networks.
  - The Executive Branch should issue an executive order detailing a structure for agency implementation and delineate responsibilities and key milestones.
- Broadband Communications Reliability and Resiliency
  - In early 2011 the Commission will begin an inquiry proceeding to gain a better understanding of the explicit and implicit standards of reliability and resiliency being applied to broadband networks.
    - The proceeding will examine the standards and practices applied to broadband infrastructure at all layers, from applications to facilities.
    - Its objective will be to determine what action, if any, the Commission should take to bolster the reliability of broadband infrastructure.

Thank You!

Questions?

Jennifer A. Manner

jennifer.manner@fcc.gov

202-418-3619

BROADBAND.GOV
NATIONAL BROADBAND PLAN